- **Procedimiento N.º: E/09545/2020**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por CODERE S.A, en el que informan a la Agencia Española de Protección de Datos que, en fecha 13 de noviembre de 2020, el Departamento de Seguridad de la Información de CODERE identificó, en la herramienta de monitorización de rendimiento de la infraestructura virtual y bases de datos, tres consultas realizadas por un usuario desconocido a las cuentas de jugadores online, pudiendo constituir una brecha de confidencialidad de los datos personales tratados bajo la responsabilidad de CODERE.

En la investigación interna realizada por el equipo de CODERE, se pudo detectar que el incidente pudo tener su origen el día 3 de noviembre de 2020.

Las consultas han sido: *jugador activo con saldo en cuenta menor o igual a 5.000* (en moneda local), *jugador activo con saldo en cuenta mayor o igual a 5.000*, consulta de *jugadores activos* donde se visualizan 7 campos de los ya consultados con anterioridad.

Han podido verse afectados los datos personales unos 590.000 clientes: código de usuario, contraseña encriptada, DNI, nacionalidad, país de residencia, nombre y apellidos, datos de localización y contacto (dirección postal, dirección de correo electrónico, teléfono), profesión, saldos en cuenta, número de cuenta bancaria.

No tienen previsto comunicar la brecha a los afectados.

CODERE manifiesta que inmediatamente procedieron a bloquear el usuario desconocido que realizó la consulta y comprobaron que se trata de un usuario con permiso de lectura que realizó las consultas desde la máquina ***XX.XX.XXX.XX***, ubicada en el data center de respaldo de ******EMPRESA.1.***

Asimismo, se activa un servicio de Ciber Vigilancia, contratado con ******EMPRESA.1***, para monitorizar el espacio web con el fin de detectar a tiempo algún tipo de exposición y se bloquea la modificación de datos personales.

Han aportado el documento "*Protocolo para la Gestión y Notificación de Brechas de Seguridad de CODERE*".

SEGUNDO: En fecha 20 de noviembre de 2020, la Directora de la Agencia Española de Protección de Datos ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: 16 de noviembre de 2020.

ENTIDADES INVESTIGADAS

CODERE, S.A., con NIF A82110453, y domicilio en Avda. de Bruselas nº 26, 28108 Alcobendas (Madrid).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En fecha 23 de noviembre, CODERE recibió Orden de la Directora de la Agencia Española de Protección de Datos obligando a comunicar a los afectados la brecha de seguridad y con fecha 19 de diciembre, CODERE remite escrito a la Agencia con las siguientes consideraciones:

- La base de datos de los jugadores de apuestas online tiene un total de 599.556 usuarios registrados. En un inicio se consideró que potencialmente podrían estar todos ellos afectados.
- Los datos de los usuarios están registrados bajo dos diferentes tipos de bases de datos, conforme a la licencia de juegos por zonas geográficas. Una base de datos "*Nacional*", dado que la licencia se aplica en todo el territorio español, con 582.259 usuarios, y otra base de datos "*Madrid*", ya que la licencia de juegos es aplicable sólo a la ciudad de Madrid, con 17.297 usuarios. Esta última base de datos está inactiva desde hace dos años. Lo que conlleva a que las cuentas de usuarios bajo esta categoría estaban inactivas y no operativas, no pudiéndose acceder.
- En la auditoría externa realizada por ******EMPRESA.2*** se comprueba que el número total de usuarios con posible exposición del dato de "*Cuenta Bancaria*" son alrededor de 60.000 usuarios y quienes tenían cumplimentado el dato de "*Profesión*" son alrededor de 40.000 usuarios. Por último, el número de usuarios en los que concurren ambos datos son 12.976 usuarios.
- Además de las medidas de seguridad implantadas con anterioridad a la brecha y las inmediatamente tomadas para minimizar el impacto no se ha detectado ninguna exposición de los datos personales de los posibles afectados y no se ha recibido ninguna queja de datos personales expuestos. Asimismo, no se han detectado anomalías en el servicio online ni actividades sospechosas en las cuentas de los usuarios. Del mismo modo, tampoco se ha recibido ninguna demanda de rescate de datos o extorsión.
- Se identificaron dos tipos de riesgos: uso no autorizado de la información con objeto de acceder a la cuenta de los usuarios en el sistema de apuestas y uso no autorizado de la información para acceder o realizar actividades financieras en cuentas bancarias externas de los usuarios.

  Teniendo en cuenta que las contraseñas están cifradas se realizó una evaluación de intento de forzar las contraseña por medio de técnicas de fuerza bruta.

  Se realizó también un análisis y evaluación más profunda del nivel de potencial peligrosidad y posible impacto sobre los usuarios de la base de datos en caso de exposición de sus cuentas de banco comprobando que en las consultas realizadas por el tercero en ningún momento se buscó o pidió tener acceso a

datos financieros de cualquier tipo, incluyendo número de cuentas de banco u otra información financiera similar. Por ello, se considera que el riesgo era sustancialmente menor del inicialmente temido.

- CODERE considera con la argumentación anterior que el número de afectados sería de unos 60.000 y para la notificación individual solicita una ampliación del plazo de comunicación a los afectados.

Con fecha 11 de enero de 2021, CODERE remite a la Agencia un nuevo escrito en el que se notifica el cumplimiento de la orden de la Directora de comunicación a los afectados. Es este escrito, mediante declaración jurada, CODERE expone:

- De acuerdo con la nueva información se ha considerado que el número de posibles afectados que han visto expuestos datos personales, como números de cuenta bancaria y profesiones, son 64.281.
- Entre las fechas 26 y 28 de diciembre de 2020 fueron notificados, por correo electrónico, los 64.281 afectados en dos etapas.
    - 1ª etapa: El usuario recibe un correo electrónico informándole que "*hemos sufrido una consulta no autorizada a nuestra base de datos*" y se le abre un enlace para recibir más información en la web, iniciando sesión como usuario.

      CODERE ha aportado texto del correo electrónico en el que se informa de la brecha, de la política de seguridad y contraseñas informando que en breve se solicitará el cambio de contraseña, todo ello con enlaces "*clic aquí*". (Apéndice I).
    - 2ª etapa: El enlace remite al usuario a su página web de inicio de sesión en el sistema, donde se le pedirá su nombre de usuario y contraseña para iniciar sesión. Una vez que el usuario inicie sesión, accede automáticamente a la carta de comunicación.

      CODERE ha aportado carta de comunicación donde se explica la brecha, y se asegura que el acceso indebido no interfiere con los fondos de los depósitos en la cuenta (Apéndice II).

Con fecha 25 de noviembre de 2020, se solicitó información a CODERE.

De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- *CODERE*, es una multinacional española en el sector del juego privado.
- CODERE no subcontrata ni externaliza el mantenimiento de los Sistemas de Información afectados por la brecha. Si bien, la ubicación del servidor (propiedad de ******EMPRESA.1***) se encuentra en un Data Center de dicha entidad.

Respecto de la cronología de los hechos. Medidas de minimización del impacto

- El 13/11/2020, el administrador de Bases de Datos detecta una consulta sospechosa sobre la Base de Datos que aloja los datos de los clientes.

  Se detecta que la consulta no es realizada por personal de CODERE y se ejecutan las consultas (*queries*) utilizadas por un supuesto atacante aplicando

los mismos filtros. Se sospecha que el servidor está comprometido y se identifica el usuario que ha lanzado las consultas.

Se bloquea inmediatamente a este usuario.

Se convoca reunión para la revisión del incidente y se definen los planes de acción a seguir, entre ellos:

- Se procede a la gestión del cambio de contraseñas de los jugadores a pesar de que las contraseñas están encriptadas.
- Se impide la modificación de datos personales (mail y número de móvil) de los jugadores para evitar suplantación de identidad.
- Se procede al clonado del servidor y se revisan todos los servidores de apuestas.
- Se implanta una herramienta de detección y respuesta.
- Se monitoriza la actividad de la base de datos con el fin de identificar patrones anómalos.

- El 15/11/2020 se estudia la posibilidad de una brecha de seguridad.
- El 16/11/2020 se notifica la brecha a la Agencia Española de Protección de Datos.
- El 17/11/2020 se procede a realizar varios envíos al equipo de Ciberseguridad con el fin de continuar con el análisis forense;
  - Imagen del disco del servidor presuntamente afectado.
  - Logs de seguridad perimetral relativos al servidor para el rango de tiempo comprendido entre el 26 de octubre y el 10 de noviembre de 2020.
  - Envío de la consulta ilegítima realizada a la base de datos.
  - Envío de la dirección IP pública del servidor afectado,
- El 20/11/2020 se enviaron además los logs correspondientes al día 3 de noviembre.

A este respecto, CODERE ha aportado informe sobre la brecha (documento nº1) y actas de las reuniones mantenidas por los responsables de la entidad (documentos del nº 2 al nº5)

Respecto de las causas que hicieron posible la brecha

- CODERE manifiesta que según el estudio de la empresa ******EMPRESA.3*** que ha realizado un análisis perimetral, la causa más probable que permitió el acceso se pudo producir a través de un servidor expuesto al exterior con una vulnerabilidad que permite lanzar comandos Powershell (la herramienta *****APLICACIÓN.1** es un recurso de entrada para el sistema operativo Windows).

  CODERE manifiesta que tenían instalado en todos los servidores una herramienta de defensa y destacan que la gestión de vulnerabilidades se hace

de manera continua sobre una muestra representativa de servidores críticos y este servidor no estaba en el grupo al que se hacía revisión continua.

- CODERE ha aportado Informe Forense realizado por ******EMPRESA.2*** como entidad de ciberseguridad. En dicho informe se concluye:
    - Se han identificación la ejecución de consultas SQL realizadas a través de un comando de Powershell codificado.
    - Se ha identificado una ejecución exitosa de las consultas ilegítimas.
    - Se han identificado comunicaciones exitosas con dos diferentes direcciones IP de índole maliciosa relacionadas con la red Tor (red que permite el anonimato a nivel de red y da acceso a la dark web)

Medidas para la resolución final de la brecha

- CODERE ha aportado informe sobre las medidas técnicas implantadas como consecuencia de la brecha, (documento nº 9), a los efectos de mitigar el impacto para los interesados y gestionar el incidente para evitar que se pueda repetir, entre ellas:
    - Mejora en las capacidades de detección mediante la implantación de una herramienta de detección y respuesta.
    - Bloqueo de la red TOR.
    - Mejoras en la monitorización ampliando los casos de uso para que se incluyan las técnicas utilizadas que provocaron la presente brecha.
    - Mejoras en la gestión de vulnerabilidades.
    - Mejoras en la configuración de la herramienta para administrar las cuentas privilegiadas, con el objetivo de proteger los activos críticos.
    - Revisión de todos los servidores de Apuestas Deportivas que han podido ser afectados, se descarta que hay otros servidores comprometidos.
    - Reinstalación y bastionado del servidor afectado.

Respecto de los datos afectados.

- El número de usuarios afectados por la brecha son unos 599.556 usuarios, aunque sólo en un 11% de los registros se incluían datos sensibles (como número de cuenta bancaria) (documento nº 7).
- Las tipologías de datos afectados son las siguientes:
    - Datos Identificativos 599.556 usuarios.
    - Datos económico-financieros (cuenta bancaria) 63.734 usuarios
    - Datos sobre circunstancias sociales (profesión) 40.186 usuarios. A este respecto CODERE manifiesta que, en muchos casos, la información registrada en este campo no corresponde al dato real de profesión, sino que es manifiestamente falsa o errónea, y no constituye, por tanto, dato personal.

- Respecto de las posibles consecuencias para los afectados, CODERE ha aportado un informe elaborado con el objeto de valorar el impacto de la brecha y mitigar sus consecuencias (documento nº 8). En dicho documento se expone:
    - Las contraseñas de todos los usuarios registrados en la base de datos son ilegibles y encriptadas.
    - La probabilidad de conseguir por técnicas de fuerza bruta superar las contraseñas es muy remota. Las condiciones de contraseñas utilizadas por la entidad están conformes a la certificación ISO 27001.
    - En el análisis y evaluación del nivel de potencial peligrosidad y posible impacto sobre los usuarios de la base de datos en caso de exposición de sus cuentas de banco se encontró que en las tres consultas ilegítimas en ningún momento se buscó o pidió tener acceso a datos financieros de cualquier tipo, incluyendo número de cuentas de banco u otra información financiera similar.
    - La base de datos no contiene copias de cualquier documento de identidad.
    - Antes del incidente se aplicaban medidas técnicas y organizativas de protección conforme a las normas ISO 27001.
    - Inmediatamente se procedió a realizar medidas apropiados para que disminuya el posible riesgo para los usuarios.
    - Desde la brecha se ha constatado la ausencia de cualquier incidente a alguno de los usuarios potencialmente afectados. Asimismo, tampoco se han detectado anomalías en el curso ordinario del negocio en línea o actividades sospechosas en las cuentas de los usuarios registrados.
    - CODERE no ha recibido ninguna demanda de rescate de datos o carta extorsión.
    - CODERE contrató los servicios de vigilancia en redes para la posible detección de la publicación de la información afectada por la brecha sin obtener datos de que se hubiera producido tal publicación en *Deep/dark web.*
- Una vez que se ha podido determinar el alcance definitivo de usuarios afectados y las tipologías de datos asociadas a los mismos, y en virtud de la Orden de comunicación a los afectados emitida por la Directora de la Agencia se procedió a la comunicación a los afectados delimitados con anterioridad a la fecha límite del 11 de enero de 2021.

<u>Respecto de las medidas de seguridad implantadas con anterioridad la brecha</u>

- CODERE ha aportado "*Certificado de Sistema de Seguridad de la Información"* emitido a favor de la organización por AENOR conforme a la Norma UNE-ISO/IEC 27001:2014 con fecha de primera emisión el 25/06/2020 y fecha de expiración el 12/07/2023 y certificado internacional en las mismas fechas. (documento nº12 y documento nº13).
- CODERE ha aportado los siguientes documentos:

- Registro de Actividad y Análisis de Riesgo de los tratamientos afectados por la brecha notificada." *Gestión de juegos online: slots y casino online"* (documento nº 11).
- Política de seguridad de la información (documento nº 14).
- Procedimiento de gestión de vulnerabilidades (documento nº 15).
- Procedimiento de gestión de ciberincidentes (documento nº 16).
- Renovación de la certificación ISO-IEC 27001 de seguridad de la información, tras una auditoría realizada y certificada por AENOR (documento nº 17 y 18).
- Informe Auditoría Interna. Nivel de adecuación al Reglamento Europeo de Protección de Datos (RGPD) en España de fecha 1 de marzo de 2018. (documento nº 19)
- Informe Seguimiento. Nivel de adecuación al RGPD en España de fecha 4 de marzo de 2020. (documento nº 20).
- Protocolo para la Gestión y Notificación de Brechas de Seguridad de Datos Personales. (aportado en la notificación de la brecha a la Agencia).
- Procedimiento de actuación del Seguro de Ciber Riesgos.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

- CODERE manifiesta que se han producido con anterioridad intentos de vulneración de la seguridad de la información de CODERE, sin embargo, es la primera ocasión en la que se produce una brecha de seguridad de datos personales.

Respecto de la notificación de brecha ante la Agencia

- CODERE manifiesta que la detección de la brecha tuvo lugar el día 13 de noviembre, pero hasta el lunes 16 de noviembre no se ha podido determinar el alcance e impacto del incidente, por lo que la notificación se presenta dentro del plazo de 72 horas que exige la Ley.

## FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación, la Directora de la Agencia Española de Protección de Datos.

II

El artículo 4 del RGPD, en su apartado 12, establece que a efectos del presente Reglamento se entenderá por *«violación de la seguridad de los datos personales»:*

*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."*

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, como consecuencia de un acceso indebido a datos personales de los clientes. Este acceso fue detectado como resultado de una consulta sospechosa sobre la base de datos.

En el presente caso, tras el requerimiento de información llevado a cabo por la inspección de esta AEPD, la entidad investigada ha informado de las investigaciones internas realizadas y del resultado de estas.

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados, pero, sin embargo, se produjo la incidencia ahora analizada, como consecuencia de la vulnerabilidad de un servidor expuesto al exterior. Se debe tener en cuenta que, si bien tenían instalados en todos los servidores una herramienta de defensa, y la gestión de vulnerabilidades se hacía de manera continua sobre una muestra representativa de servidores críticos, este servidor no estaba en el grupo al que se hacía la revisión continua. Por otro lado, aporta el "Certificado de Sistema de Seguridad de la Información" emitido a favor de la organización por AENOR conforme a la Norma UNE-ISO/IEC 27001, así como el Registro de Actividad y Análisis de Riesgo de los tratamientos afectados por la brecha notificada.

Asimismo, contaba con protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

Se debe destacar la rápida actuación de la entidad desde el mismo momento en que tuvo conocimiento de los hechos, interviniendo de forma activa en su resolución, minimizando los posibles efectos perniciosos del incidente, e implementando contramedidas que bloquearon de forma inmediata al usuario.

No constan reclamaciones ante esta Agencia por parte de terceros. Tampoco se han detectado incidentes ni anomalías en el curso ordinario del negocio en línea o actividades sospechosas en las cuentas de los usuarios registrados.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente. Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá

para prevenir la reiteración de una brecha de similares características como la analizada.

III

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de la entidad investigada como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a CODERE, S.A.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-0419

Mar España Martí
Directora de la Agencia Española de Protección de Datos